Fig.1: Placement for the Invention Apparatus in an Organization to stop intrusions
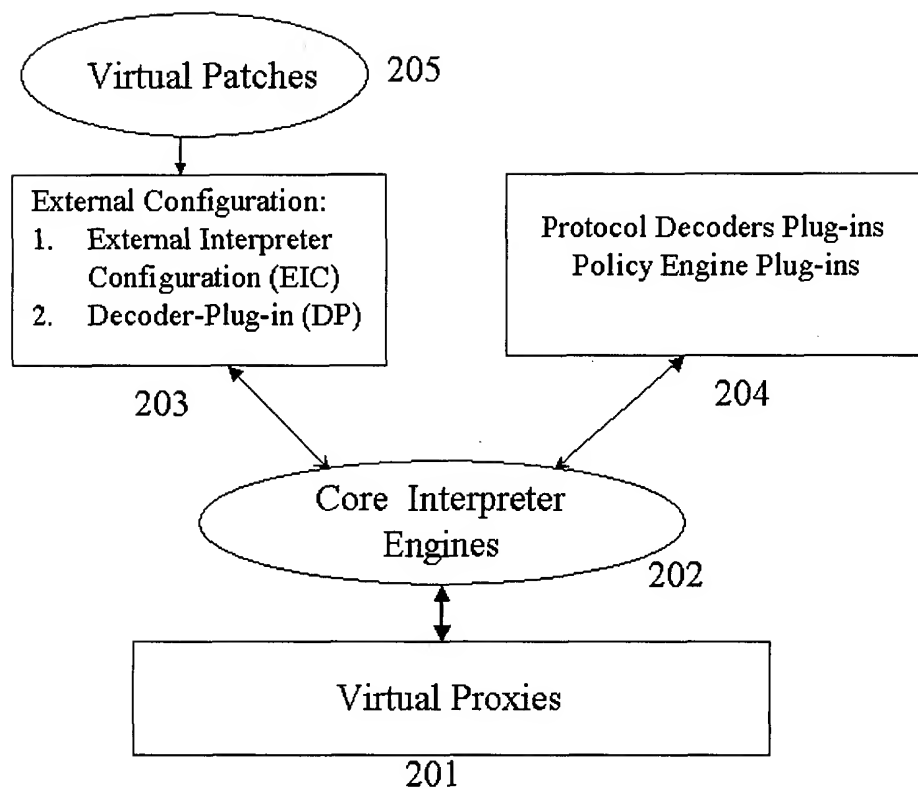
Fig.2: Primary elements of the apparatus and method for stopping intrusion

External Configuration:
1. External Interpreter
   Configuration (EIC)
2. Decoder-Plugin (DP)

Built-in Decoder or
Auto-learned Policy
Plugins

Core Interpreter Engine

Access
Policy

Engine

TCP/IP

Interceptors

Application

Virtual
Proxy

301

302

303

Fig.3: Primary elements of a network based apparatus that uses this invention

```
┌─────────────────────────────┐        ┌─────────────────────────────┐
│ External Configuration:     │        │    Built-in Decoder or      │
│ 1.  External Interpreter    │        │   Auto-learned Policy       │
│     Configuration (EIC)     │        │        Plugins              │
│ 2.  Decoder-Plugin (DP)     │        │                             │
└─────────────────────────────┘        └─────────────────────────────┘
```

Core Interpreter Engine

```
┌──────────┐  ┌────────────┐  ┌──────────────────┐   ┌──────────────┐
│          │  │            │  │ External Module: │   │              │
│          │  │  TCP/IP    │  │   Application    │   │ Application  │
│  Access  │  │            │  │    Specific      │   │              │
│  Policy  │  │            │  │   Processing     │   │              │
│          │  │            │  │                  │   │              │
│  Engine  │  │ Interceptors│ │   Ex: SQL        │   │  Virtual     │
│          │  │            │  │   Transport      │   │  Proxy       │
│          │  │            │  │    Layer         │   │              │
└──────────┘  └────────────┘  └──────────────────┘   └──────────────┘
    401            402              403                    404
```

Fig.4: Primary elements of a host based apparatus that uses this invention

Interpreter Configuration Structure (ICS)

•Semantic tree structures and their roots
•Root decoding procedures for client and server
•Protocol level parameters that control decoder plug-in
•Additional protocol level parameters that control processing vulnerabilities, exposures, and policies
•List of application information elements that decoder plug-in should extract.
•Procedures used to process events when exceptions are detected by the decoder
•Procedures used to initialize a session context
•Procedures to free-up storage for a session context
•Procedure to free-up memory when the interpreter configuration data structure is removed
•Compiled set of regular expressions, pattern lists, and value lists
•A reference count

501

External Interpreter Configuration (EIC)

•Procedure to enhance or change semantic trees
•Procedure to change protocol level parameters that control decoder plugin
•Protocol level parameters that control processing of vulnerabilities, exposures, and policies
•List of application information elements that decoder plug-in should extract.
•Changes to the procedures used to process events when exceptions are detected by the decoder
•Procedure used to initialize session context related to processing of vulnerabilities, exposures, and policies
•Procedure used to free external session context
•Procedures for processing vulnerabilities, exposures, and policies
•Compiled Regular expressions, pattern lists, and value lists

502

Decoder Plug-in (DP)

•Procedure to build semantic trees
•Root decoding procedures for client and server
•Protocol level parameters that control decoder plug-in
•Procedures used to process events when exceptions are detected by the decoder
•Procedure used to initialize decoder related session context
•Procedure used to free decoder related session context
•Procedure to create a data structure which contains all information elements that can be enabled for decoding
•Procedures for decoding information elements and maintaining session context related to decoder session context
•Procedure for inserting decoding procedures into semantic trees

503

Fig.5: Using EIC and DP to build ICS

Dynamic Elements (IEs/SPs)   Semantic Trees

601   IE (A)   602   SSEA

IE1(B)   IE2(C)   IE3(C)   SSEB   SSEC
603   604   605   606   607

608   Session Context   Null Session Root 614

SP1 (P) SP2(Q) SP3(Q)   SSEP   SSEQ
609   610   611   612   613

Fig. 6: Relationship between dynamic application elements and semantic trees

	2002	2001	2000
CVE Count	1307	1506	990

Figure 7: Total CVE count on yearly basis

801	802	803	804
Decoding Constructs	Protocol Level Context	Session State Context	Vulnerability, Exposure Semantics

EBNF Type 805   3G Like 806

For Decode Procedures 807

For vulnerability and exposure processing 808

For vulnerability and exposure processing 809

810 Validation Construct

811 Action Construct

812

Length Check
Regexp Match
Value Check
Value List Check
Char Set Check
Tag Comp Check
Invalid Content
DOS Control
3G-like Construct

813

Alert, Log
Audit
Remove-MC
Normalize-MC
Insert New Cont
App Specific

Figure 8: Elements of a method and apparatus for capturing vulnerabilities/exposures.